Finite Fields and Their Applications 18 (2012) 56–62

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A note on linearized polynomials and the dimension of their kernels

San Ling [a,1], Longjiang Qu [b,a,*,2]

[a] Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore
[b] Department of Mathematics and System Science, Science College, National University of Defense Technology, ChangSha, 410073, China

ARTICLE INFO

Article history:
Received 1 May 2011
Revised 8 June 2011
Accepted 16 June 2011
Available online 2 July 2011
Communicated by L. Storme

MSC:
11T06

Keywords:
Linearized polynomials
Kernel
Finite field

ABSTRACT

Recently explicit representations of the class of linearized permutation polynomials and the number of such polynomials were given in Zhou (2008) [4] and Yuan and Zeng (2011) [3]. In this paper, we generalize this result to linearized polynomials with kernel of any given dimension, solving an open problem in Charpin and Kyureghyan (2009) [1]. Moreover, more explicit representations of such polynomials are given and several classes of explicit linearized polynomials with kernel of any given dimension are presented.

1. Introduction

Let q be a prime power, let $\mathbb{F}_q$ be the finite field of order q, and let $\mathbb{F}_q[x]$ be the ring of polynomials in a single indeterminate x over $\mathbb{F}_q$. An interesting class of polynomials over finite fields is the class of linearized polynomials. Let n be a positive integer, a polynomial of the form

* Corresponding author at: Department of Mathematics and System Science, Science College, National University of Defense Technology, ChangSha, 410073, China.
E-mail addresses: lingsan@ntu.edu.sg (S. Ling), ljqu_happy@hotmail.com (L.J. Qu).

[1] The work of S. Ling is supported by the Singapore National Research Foundation Competitive Research Program grant NRF-CRP2-2007-03.
[2] The work of L.J. Qu is supported by the NSFC of China under Grant 60803156, and the Singapore National Research Foundation Competitive Research Program grant NRF-CRP2-2007-03.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.06.002

$$L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$$

is called a q-polynomial (or a linearized polynomial) over $\mathbb{F}_{q^n}$.

A polynomial $f \in \mathbb{F}_q[x]$ is called a permutation polynomial if it induces a one-to-one mapping from $\mathbb{F}_q$ to itself. In recent years, there has been much interest in constructing permutation polynomials over finite fields, due to their applications in combinatorics, cryptography and coding theory. Linearized permutation polynomials have been paid particular attention. Explicit representations of the class of linearized permutation polynomials and their number have been given by K. Zhou [4], P.Z. Yuan and X.N. Zeng [3].

Linearized permutation polynomials are linear mappings with kernel of dimension 0. However, linearized polynomials with kernel of other dimensions have not been well classified yet. Recently, P. Charpin and G. Kyureghyan used linearized polynomials with kernel of dimension 1 to construct permutation polynomials, and they raised the following problem [1].

Open Problem. *Find classes of linearized polynomials over $\mathbb{F}_{q^n}$ describing mappings with kernel of dimension* 1.

In this note, we give several explicit representations and the number of linearized polynomials with kernel of any given dimension, which generalizes the theorems in [3] and solves the above open problem.

We end this introduction with some notations. For positive integers m and n, the space of $m \times n$ matrices over $\mathbb{F}_q$ is denoted by $\mathbb{F}_q^{m\times n}$. For any matrix A over $\mathbb{F}_q$, $\mathrm{Rank}_{\mathbb{F}_q}(A)$ denotes the rank of A. For a set of vectors $\{v_1, \ldots, v_r\}$ of the same length over $\mathbb{F}_q$, $\mathrm{Span}(v_1, \ldots, v_r)$ denotes the vector space spanned by $\{v_1, \ldots, v_r\}$, and $\mathrm{Rank}_{\mathbb{F}_q}\{v_1, \ldots, v_r\}$ is the dimension of $\mathrm{Span}(v_1, \ldots, v_r)$. The trace function $\mathrm{Tr}(x)$ from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is defined by

$$\mathrm{Tr}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{n-1}}.$$

For a mapping L, $\mathrm{Ker}(L)$ denotes the kernel of L while $\mathrm{Im}(L)$ is its image set.

2. Main results

The following lemma is needed in the rest of the paper. It is an old result with the first derivation of the formula due to Landsberg (1893) [2, p. 455]. However, we include here a short proof for the readers' convenience.

Lemma 2.1. *Let m, n, k be positive integers, $k \leqslant \min\{m, n\}$, $S_k(m, n) = \{A \in \mathbb{F}_q^{m\times n}\colon \mathrm{Rank}_{\mathbb{F}_q}(A) = k\}$, then* $|S_k(m, n)| = \frac{\prod_{i=0}^{k-1}(q^m-q^i)(q^n-q^i)}{\prod_{i=0}^{k-1}(q^k-q^i)}$.

Proof. Let A be an element of $S_k(m, n)$, $A = [\alpha_1, \alpha_2, \ldots, \alpha_n]$, $\alpha_i \in \mathbb{F}_q^m$, $V = \mathrm{Span}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq \mathbb{F}_q^m$, then V is a subspace with dimension k. It is clear that there are $\frac{\prod_{i=0}^{k-1}(q^m-q^i)}{\prod_{i=0}^{k-1}(q^k-q^i)}$ different subspaces with dimension k in $\mathbb{F}_q^m$. Once a k-dimensional subspace V is fixed, we need to choose n vectors with rank k from V to construct A. Let $\{\beta_1, \beta_2, \ldots, \beta_k\}$ be a basis of V over $\mathbb{F}_q$, then there exists a unique $k \times n$ matrix B over $\mathbb{F}_q$ with rank k such that $A = [\beta_1, \beta_2, \ldots, \beta_k]B$. The number of matrices of size $k \times n$ with rank k over $\mathbb{F}_q$ is $\prod_{i=0}^{k-1}(q^n - q^i)$. Hence, $|S_k(m, n)| = \frac{\prod_{i=0}^{k-1}(q^m-q^i)}{\prod_{i=0}^{k-1}(q^k-q^i)} \cdot \prod_{i=0}^{k-1}(q^n - q^i) = \frac{\prod_{i=0}^{k-1}(q^m-q^i)(q^n-q^i)}{\prod_{i=0}^{k-1}(q^k-q^i)}$. □

Now we can introduce our first two results.

Theorem 2.2. *Let $\{\beta_1, \beta_2, \ldots, \beta_n\}$ be any given basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and let $L(x)$ be a linearized polynomial over $\mathbb{F}_{q^n}$. Then there exists a unique vector $(\theta_1, \theta_2, \ldots, \theta_n) \in \mathbb{F}_{q^n}^n$ such that*

$$L(x) = \mathrm{Tr}(\theta_1 x)\beta_1 + \cdots + \mathrm{Tr}(\theta_n x)\beta_n = \sum_{i=0}^{n-1}\left(\sum_{j=1}^{n}\beta_j\theta_j^{q^i}\right)x^{q^i}. \tag{1}$$

Moreover, let k be an integer such that $0 \leqslant k \leqslant n$, then $\dim_{\mathbb{F}_q}(\mathrm{Ker}(L)) = k$ if and only if $\mathrm{Rank}_{\mathbb{F}_q}\{\theta_1, \theta_2, \ldots, \theta_n\} = n - k$. In particular, $k = n$ if and only if $L(x) \equiv 0$. If $k < n$, then there are exactly $\frac{\prod_{i=0}^{n-k-1}(q^n - q^i)^2}{\prod_{i=0}^{n-k-1}(q^{n-k} - q^i)}$ different linearized polynomials with kernel of dimension k.

Proof. The first part of the theorem has been proved in [3]. We only prove the second part.

Let $W = \mathrm{Span}(\theta_1, \ldots, \theta_n)$ be the $\mathbb{F}_q$-subspace generated by $\theta_1, \ldots, \theta_n$, and let $W^\top = \{x \in \mathbb{F}_{q^n}: \mathrm{Tr}(\theta x) = 0 \text{ for every } \theta \in W\}$. Then

$$\mathrm{Ker}(L) = \left\{x \in \mathbb{F}_{q^n}: \mathrm{Tr}(\theta_i x) = 0,\ 1 \leqslant i \leqslant n\right\} = W^\top.$$

Since $\langle x, y\rangle = \mathrm{Tr}(xy)$ is a non-degenerate bilinear form $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \to \mathbb{F}_q$, it follows that

$$\dim_{\mathbb{F}_q} W^\top = n - \dim_{\mathbb{F}_q} W.$$

Then

$$\dim_{\mathbb{F}_q} \mathrm{Ker}(L) = \dim_{\mathbb{F}_q} W^\top = n - \dim_{\mathbb{F}_q} W = n - \mathrm{Rank}_{\mathbb{F}_q}\{\theta_1, \theta_2, \ldots, \theta_n\}.$$

Thus $\dim_{\mathbb{F}_q}(\mathrm{Ker}(L)) = k$ if and only if $\mathrm{Rank}_{\mathbb{F}_q}\{\theta_1, \theta_2, \ldots, \theta_n\} = n - k$. It is clear that $\dim_{\mathbb{F}_q}(\mathrm{Ker}(L)) = k = n$ if and only if $L(x) \equiv 0$. If $k < n$, then the number of linearized polynomials with kernel of dimension k is the number of vector sets $\{\theta_1, \theta_2, \ldots, \theta_n\} \subset \mathbb{F}_{q^n}$ with rank $n - k$ over $\mathbb{F}_q$, which is $S_{n-k}(n, n)$. The desired result now follows from Lemma 2.1. □

Theorem 2.3. *Let $\{\theta_1, \theta_2, \ldots, \theta_n\}$ be any given basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and let $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ be a linearized polynomial over $\mathbb{F}_{q^n}$.*

1. *Then there exists a unique vector $(\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{F}_{q^n}^n$ such that*

$$L(x) = \mathrm{Tr}(\theta_1 x)\beta_1 + \cdots + \mathrm{Tr}(\theta_n x)\beta_n = \sum_{i=0}^{n-1}\left(\sum_{j=1}^{n}\beta_j\theta_j^{q^i}\right)x^{q^i}. \tag{2}$$

2. *Let $D = [d_{i,j}]_{n\times n}$ be a square matrix of size n over $\mathbb{F}_{q^n}$, where $d_{i,j} = \theta_j^{q^{i-1}}$, $1 \leqslant i, j \leqslant n$. Then D is invertible and*

$$(\beta_1, \beta_2, \ldots, \beta_n)^{\mathrm{T}} = D^{-1}(a_0, a_1, \ldots, a_{n-1})^{\mathrm{T}}, \tag{3}$$

   where $^{\mathrm{T}}$ denotes the transpose.
3. *Let k be an integer such that $0 \leqslant k \leqslant n$. Then $\dim_{\mathbb{F}_q}(\mathrm{Ker}(L)) = k$ if and only if $\mathrm{Rank}_{\mathbb{F}_q}\{\beta_1, \beta_2, \ldots, \beta_n\} = n - k$.*

Proof. 1. Define a linear mapping from $\mathbb{F}_{q^n}^n$ to $\mathbb{F}_{q^n}[x]$ as follows:

$$\phi : \beta = (\beta_1, \beta_2, \ldots, \beta_n) \to L_\beta(x) = \mathrm{Tr}(\theta_1 x)\beta_1 + \cdots + \mathrm{Tr}(\theta_n x)\beta_n.$$

It is clear that $L_\beta(x)$ is a linearized polynomial over $\mathbb{F}_{q^n}$. Since $\{\theta_1, \theta_2, \ldots, \theta_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, by Theorem 2.2 we know that $(\mathrm{Tr}(\theta_1 x), \mathrm{Tr}(\theta_2 x), \ldots, \mathrm{Tr}(\theta_n x))$ runs through all the vectors of $\mathbb{F}_q^n$ when x runs over $\mathbb{F}_{q^n}$. Thus ϕ is an injective mapping from $\mathbb{F}_{q^n}^n$ into the set of linearized polynomials over $\mathbb{F}_{q^n}$. Then, with the fact that both of these sets have the same cardinality, i.e., q^{n^2}, we have that ϕ is a bijective mapping, which proves the first part.

2. From (2), we have

$$a_i = \sum_{j=1}^{n} \beta_j \theta_j^{q^i}, \quad 0 \leqslant i \leqslant n-1. \tag{4}$$

Writing the above formula into matrix form, we get

$$(a_0, a_1, \ldots, a_{n-1})^{\mathrm{T}} = D(\beta_1, \beta_2, \ldots, \beta_n)^{\mathrm{T}}.$$

Since $\{\theta_1, \theta_2, \ldots, \theta_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, D is invertible [2, Corollary 2.38], and (3) follows.

3. For the proof of the last part, first note that $\dim_{\mathbb{F}_q}(\mathrm{Ker}(L)) = k$ if and only if $\dim_{\mathbb{F}_q}(\mathrm{Im}(L)) = n-k$. Then since $L(x)$ runs over all the $\mathbb{F}_q$-linear combinations of $\beta_1, \beta_2, \ldots, \beta_n$ when x runs over $\mathbb{F}_{q^n}$, we have $\dim_{\mathbb{F}_q}(\mathrm{Im}(L)) = \mathrm{Rank}_{\mathbb{F}_q}(\beta_1, \beta_2, \ldots, \beta_n)$. The theorem is thus proved. □

Theorems 2.2 and 2.3 give two explicit representations of linearized polynomials with kernel of any given dimension. With either of them, one can construct linearized polynomials with kernel of any desired dimension. Further, all such polynomials can be constructed this way since the conditions in the theorems are both sufficient and necessary.

Both the formulas in Theorems 2.2 and 2.3 involve $2n$ vectors, including a basis and a set of n vectors with given rank. We can reduce the number of vectors needed from $2n$ to $2(n-k)$ for linearized polynomials with kernel of dimension k.

Theorem 2.4. *Let $L(x)$ be a linearized polynomial over $\mathbb{F}_{q^n}$, and let k be an integer such that $0 \leqslant k \leqslant n$. Then $\dim_{\mathbb{F}_q}(\mathrm{Ker}(L)) = k$ if and only if there exist two vector sets over $\mathbb{F}_{q^n}$ with rank $n-k$ over $\mathbb{F}_q$, $\{\omega_1, \omega_2, \ldots, \omega_{n-k}\}$ and $\{\gamma_1, \gamma_2, \ldots, \gamma_{n-k}\}$, such that*

$$L(x) = \sum_{i=1}^{n-k} \mathrm{Tr}(\gamma_i x)\omega_i = \sum_{i=0}^{n-1} \left(\sum_{j=1}^{n-k} \omega_j \gamma_j^{q^i} \right) x^{q^i}. \tag{5}$$

Proof. Let $\{\theta_1, \theta_2, \ldots, \theta_n\}$ be any given basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. If $\dim_{\mathbb{F}_q}(\mathrm{Ker}(L)) = k$, then, by Theorem 2.3, there exist $\beta_1, \beta_2, \ldots, \beta_n \in \mathbb{F}_{q^n}$ with rank $n-k$ over $\mathbb{F}_q$ such that $L(x) = \sum_{i=1}^{n} \mathrm{Tr}(\theta_i x)\beta_i$. Let $\omega_1, \omega_2, \ldots, \omega_{n-k}$ be a basis of $\mathrm{Span}(\beta_1, \beta_2, \ldots, \beta_n)$, and let $\beta_j = \sum_{i=1}^{n-k} c_{i,j}\omega_i$, $c_{i,j} \in \mathbb{F}_q$, $1 \leqslant j \leqslant n$. Then we have

$$L(x) = \sum_{j=1}^{n} \mathrm{Tr}(\theta_j x) \sum_{i=1}^{n-k} c_{i,j}\omega_i = \sum_{i=1}^{n-k} \omega_i \sum_{j=1}^{n} \mathrm{Tr}(c_{i,j}\theta_j x) = \sum_{i=1}^{n-k} \omega_i \mathrm{Tr}\left(\left(\sum_{j=1}^{n} c_{i,j}\theta_j \right) x \right).$$

Let $\gamma_i = \sum_{j=1}^{n} c_{i,j}\theta_j$, $1 \leqslant i \leqslant n-k$, then we get $L(x) = \sum_{i=1}^{n-k} \mathrm{Tr}(\gamma_i x)\omega_i = \sum_{i=0}^{n-1} (\sum_{j=1}^{n-k} \omega_j \gamma_j^{q^i}) x^{q^i}$. Let $C = [c_{i,j}]_{(n-k)\times n}$, then $\mathrm{Rank}_{\mathbb{F}_q}\{\gamma_1, \gamma_2, \ldots, \gamma_{n-k}\} = \mathrm{Rank}_{\mathbb{F}_q}(C) = n-k$, which proves the necessity.

For sufficiency, it is enough to note that the above proof is reversible. □

Theorem 2.4 gives another explicit form of all linearized polynomials with kernel of any given dimension. The advantage of this form is that it needs fewer vectors compared with those in Theorems 2.2 and 2.3, which can be quite useful especially when k is close to n, i.e., where the dimension of the image is quite small. The following corollary is an example.

Corollary 2.5. *Let $L(x)$ be a linearized polynomial over $\mathbb{F}_{q^n}$. Then $\dim_{\mathbb{F}_q} \mathrm{Ker}(L) = n-1$ if and only if there exist $0 \neq \omega \in \mathbb{F}_{q^n}$ and $0 \neq \gamma \in \mathbb{F}_{q^n}$ such that*

$$L(x) = \omega \mathrm{Tr}(\gamma x) = \sum_{i=0}^{n-1} \omega \gamma^{q^i} x^{q^i}.$$

It should be noted that the representation in Theorem 2.4 is not necessarily unique. One can, however, impose some restrictions on the representation to achieve uniqueness.

Theorem 2.6. *Let $\{\theta_1, \theta_2, \ldots, \theta_n\}$ be any given basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and let k be an integer such that $0 \leqslant k \leqslant n$. Then all the linearized polynomials over $\mathbb{F}_{q^n}$ with kernel of dimension k are uniquely given by*

$$L(x) = \sum_{i=1}^{n-k} \mathrm{Tr}(\gamma_i x)\omega_i = \sum_{i=0}^{n-1} \left(\sum_{j=1}^{n-k} \omega_j \gamma_j^{q^i} \right) x^{q^i}, \tag{6}$$

where ω_i, γ_i satisfy the following conditions:

(i) *$\{\omega_1, \omega_2, \ldots, \omega_{n-k}\}$ is some vector set over $\mathbb{F}_{q^n}$ with rank $n-k$ over $\mathbb{F}_q$,*
(ii) *$\gamma_i = \sum_{j=1}^{n} c_{i,j}\theta_j$, $c_{i,j} \in \mathbb{F}_q$, $1 \leqslant i \leqslant n-k$, $1 \leqslant j \leqslant n$, where $C = [c_{i,j}]_{(n-k)\times n}$ is in reduced row echelon form of rank $n-k$.*

Proof. Let $L(x)$ be a linearized polynomial over $\mathbb{F}_{q^n}$ with kernel of dimension k. Then, by Theorem 2.3, there exist $\beta_1, \beta_2, \ldots, \beta_n \in \mathbb{F}_{q^n}$ with rank $n-k$ over $\mathbb{F}_q$ such that $L(x) = \sum_{i=1}^{n} \mathrm{Tr}(\theta_i x)\beta_i$. By Theorem 2.4 and its proof, there exists a unique matrix $C \in \mathbb{F}_q^{(n-k)\times n}$ with rank $n-k$ such that $(\gamma_1, \gamma_2, \ldots, \gamma_{n-k})^{\mathrm{T}} = C(\theta_1, \theta_2, \ldots, \theta_n)^{\mathrm{T}}$, $(\beta_1, \beta_2, \ldots, \beta_n) = (\omega_1, \ldots, \omega_{n-k})C$ and $L(x) = \sum_{i=1}^{n-k} \mathrm{Tr}(\gamma_i x)\omega_i$. We call C the matrix corresponding to such a representation.

Let $L(x) = \sum_{i=1}^{n-k} \mathrm{Tr}(\gamma_i x)\omega_i = \sum_{i=1}^{n-k} \mathrm{Tr}(\gamma_i' x)\omega_i'$ and let C and C' be their corresponding matrices, respectively. Then we have $(\omega_1, \ldots, \omega_{n-k})C = (\omega_1', \ldots, \omega_{n-k}')C'$. Since $\omega_1, \ldots, \omega_{n-k}$ and $\omega_1', \ldots, \omega_{n-k}'$ are two bases of the vector space $\mathrm{Span}(\beta_1, \beta_2, \ldots, \beta_n)$, there exists an invertible matrix P such that $(\omega_1', \ldots, \omega_{n-k}') = (\omega_1, \ldots, \omega_{n-k})P$. Then we have $C = PC'$, which is equivalent to the fact that C' can be transformed to C by elementary row transformations, or equivalently, C' and C have the same reduced row echelon form.

Let $L(x)$ be a polynomial given by (6) satisfying (i). For the matrix C corresponding to a representation of $L(x)$, let P be the unique invertible matrix such that $C = PC'$, where C' is the reduced row echelon form of C. Let $(\omega_1', \ldots, \omega_{n-k}') = (\omega_1, \ldots, \omega_{n-k})P$, and $(\gamma_1', \gamma_2', \ldots, \gamma_{n-k}')^{\mathrm{T}} = C'(\theta_1, \theta_2, \ldots, \theta_n)^{\mathrm{T}}$, then $L(x) = \sum_{i=1}^{n-k} \mathrm{Tr}(\gamma_i' x)\omega_i'$. Thus every linearized polynomial with kernel of dimension k can be given by (6) satisfying both (i) and (ii). Moreover, the expression of a polynomial given by (6), satisfying both (i) and (ii), is unique since every matrix has a unique reduced row echelon form. The proof is now completed. □

Several explicit representations of linearized polynomials with kernel of any given dimension are now given. With any of them, one can construct all such polynomials. As shown in Corollary 2.5, the forms of the linearized polynomials may be quite simple if the dimensions of their images are quite small, though it should be noted that the explicit forms of such polynomials may be quite complicated in general. However, constructions of linearized polynomials with kernel of any desired

dimension and whose coefficients can be described simply are also possible with suitable choices of the vector sets. Several classes of such polynomials are constructed as examples in the following two propositions. It is clear that if $L(x)$ is a q-polynomial over $\mathbb{F}_{q^n}$ with kernel of dimension k, then $L(ax)$ and $aL(x)$ are also such polynomials for any $a \in \mathbb{F}_{q^n}^*$. Therefore one can obtain more such functions from those given in the following propositions.

Proposition 2.7. *Let α be a primitive element of the finite field $\mathbb{F}_{q^n}$, $q^n \geqslant 5$, let k be an integer such that $0 \leqslant k < n$, let τ be a mapping from $\{0, 1, \ldots, n-1\}$ onto $\{0, 1, \ldots, n-k-1\}$, and let*

$$L_{\tau,k,1}(x) = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} \alpha^{\tau(j)\cdot q^i + j} \right) x^{q^i},$$

$$L_{\tau,k,2}(x) = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} \alpha^{j\cdot q^i + \tau(j)} \right) x^{q^i},$$

$$L_k(x) = \sum_{i=0}^{n-1} \frac{\alpha^{(n-k)(q^i+1)} - 1}{\alpha^{q^i+1} - 1} x^{q^i}.$$

Then $L_{\tau,k,1}(x)$, $L_{\tau,k,2}(x)$, $L_k(x)$ are linearized polynomials with kernel of dimension k. In particular, $L_{\tau,0,1}(x)$, $L_{\tau,0,2}(x)$, $L_0(x)$ are linearized permutation polynomials.

Proof. Let $(\beta_1, \beta_2, \ldots, \beta_n) = (1, \alpha, \ldots, \alpha^{n-1})$ and $(\theta_1, \theta_2, \ldots, \theta_n) = (\alpha^{\tau(0)}, \alpha^{\tau(1)}, \ldots, \alpha^{\tau(n-1)})$. Then $\{\beta_1, \beta_2, \ldots, \beta_n\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and $\mathrm{Rank}_{\mathbb{F}_q}(\theta_1, \theta_2, \ldots, \theta_n) = n-k$ since τ is a surjective mapping. Then, by direct computation, we have $L_{\tau,k,1}(x) = \sum_{i=1}^{n} \mathrm{Tr}(\theta_i x)\beta_i$ and $L_{\tau,k,2}(x) = \sum_{i=1}^{n} \mathrm{Tr}(\beta_i x)\theta_i$. By Theorems 2.2 and 2.3, we know that both $L_{\tau,k,1}(x)$ and $L_{\tau,k,2}(x)$ are linearized polynomials with kernel of dimension k.

Let $(\beta_1, \beta_2, \ldots, \beta_n) = (1, \alpha, \ldots, \alpha^{n-1})$ and $(\theta_1, \theta_2, \ldots, \theta_n) = (1, \alpha, \ldots, \alpha^{n-k-1}, 0, \ldots, 0)$. Then we have $L_k(x) = \sum_{i=1}^{n} \mathrm{Tr}(\theta_i x)\beta_i$. The results thus follow. □

Proposition 2.8. *Let α be a primitive element of the finite field $\mathbb{F}_{q^n}$, $q^n \geqslant 5$, let k be an integer such that $0 \leqslant k < n$, and let*

$$L_{k,1}(x) = \sum_{i=0}^{n-1} \left(\frac{\alpha^{(n-k)q^i} - 1}{\alpha^{q^i} - 1} - \frac{\alpha^{(n-k)(q^i+1)+1} - \alpha}{\alpha^{q^i+1} - 1} \right) x^{q^i},$$

$$L_{k,2}(x) = \sum_{i=0}^{n-1} \left(\frac{\alpha^{n-k} - 1}{\alpha - 1} - \frac{\alpha^{(n-k)(q^i+1)+q^i} - \alpha^{q^i}}{\alpha^{q^i+1} - 1} \right) x^{q^i}.$$

Then both $L_{k,1}(x)$ and $L_{k,2}(x)$ are linearized polynomials with kernel of dimension k. In particular, $L_{0,1}(x)$ and $L_{0,2}(x)$ are linearized permutation polynomials.

Proof. Let $(\theta_1, \theta_2, \ldots, \theta_n) = (1, \alpha, \ldots, \alpha^{n-1})$ and $(\beta_1, \beta_2, \ldots, \beta_n) = (1, 1+\alpha, \sum_{j=0}^{2} \alpha^j, \ldots, \sum_{j=0}^{n-k-1} \alpha^j, 0, \ldots, 0)$. Then, by direct computation, we have $L_{k,1}(x) = (1-\alpha)\sum_{i=1}^{n} \mathrm{Tr}(\theta_i x)\beta_i$ and $L_{k,2}(x) = \sum_{i=1}^{n} \mathrm{Tr}(\beta_i(1-\alpha)x)\theta_i$. Then the results follow by Theorems 2.2 and 2.3. □

Acknowledgments

The authors would like to thank the anonymous referees for their comments and suggestions.

References

[1] P. Charpin, G. Kyureghyan, When does $G(x) + \gamma \operatorname{Tr}(H(x))$ permute $\mathbb{F}_{p^n}$?, Finite Fields Appl. 15 (2009) 615–632.
[2] R. Lidl, H. Niederreiter, Finite Fields, second ed., Encyclopedia Math. Appl., vol. 20, Cambridge University Press, Cambridge, 1997.
[3] P. Yuan, X. Zeng, A note on linear permutation polynomials, Finite Fields Appl. 17 (5) (2011) 488–491.
[4] K. Zhou, A remark on linear permutation polynomials, Finite Fields Appl. 14 (2008) 532–536.